

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

2016 DEC 28 P 4:39

UNITED STATES OF AMERICA

v.

JUSTIN GRAY LIVERMAN,
(a/k/a "D3F4ULT")

Defendant.

Criminal No. 1:16-CR-313

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

Count 1: 18 U.S.C. § 371
Conspiracy

CRIMINAL INFORMATION

THE UNITED STATES ATTORNEY CHARGES THAT:

Count 1
Conspiracy

1. From at least in or around November 2015 through in or around February 2016, in the Eastern District of Virginia and elsewhere, defendant JUSTIN GRAY LIVERMAN, a/k/a "D3F4ULT," knowingly and intentionally agreed and conspired with ANDREW OTTO BOGGS, a/k/a "INCURSIO," and a conspirator identified herein as "CRACKA," along with other persons known and unknown to the United States Attorney, to commit offenses against the United States, namely:

(a) Identity theft, that is, to knowingly transfer, possess, and use in or affecting interstate or foreign commerce, without lawful authority, a means of identification of another person, to wit, names, usernames, unique electronic identification number and addresses, and passwords, knowing that the means of identification belonged to another actual person, with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that

constitutes a violation of Federal law, in violation of Title 18, United States Code, Section 1028(a)(7);

(b) Unauthorized access of a protected computer, that is, to intentionally access a computer without authorization and thereby obtain information from any protected computer and from any department and agency of the United States, and the offense was committed in furtherance of criminal and tortious acts in violation of the laws of the United States (including Making Public Restricted Personal Information, a violation of 18 U.S.C. § 119, Cyberstalking, a violation of 18 U.S.C. § 2261A(2), and Telephone Harassment, a violation of 47 U.S.C. § 223(a)(1)), in violation of Title 18, United States Code, Section 1030(a)(2) and (c)(2)(B); and

(c) Making harassing telephone calls, that is, in interstate or foreign communications, to utilize a telecommunications device, whether or not communication ensues, without disclosing one's identity and with intent to abuse, threaten, and harass any specific person, in violation of Title 47, United States Code, Sections 223(a)(1)(C)-(D).

Manner and Means of the Conspiracy

2. It was part of the conspiracy that members of the conspiracy targeted U.S. government officials' online accounts and government computer databases for unauthorized access for the purpose of, among other things, obtaining private, sensitive, and confidential information; making such obtained information available on public websites; and harassing and intimidating, or attempting to intimidate, victims through anonymous phone calls to victims and others whose phone numbers were located in the call records of other victims.

3. It was further part of the conspiracy that members of the conspiracy used multiple pseudonymous online accounts to communicate with co-conspirators and publicly harass victims.

4. It was further part of the conspiracy that members of the conspiracy posed as victims in communications with online and computer service providers for the purpose of attempting to obtain the victims' private information.

5. It was further part of the conspiracy that members of the conspiracy used mobile phone applications or voice over Internet Protocol technology to mask the true phone numbers from which they called, thereby masking their identities.

6. It was further part of the conspiracy that members of the conspiracy used anonymizing programs such as virtual private networks, encrypted chat programs, and the encrypted Tor browser, to conceal their true identities and locations.

7. It was further part of the conspiracy that members of the conspiracy utilized Twitter to publicly disseminate website addresses and passwords where the conspirators had uploaded their victims' private, confidential, and sensitive information.

8. It was further part of the conspiracy that members of the conspiracy used victim email addresses in communications with third parties without authorization.

9. It was further part of the conspiracy that members of the conspiracy unlawfully used a senior U.S. government official's login credentials to gain access to and attempt access to the Law Enforcement Enterprise Portal ("LEEP"), a U.S. government computer system that provided law enforcement agencies, intelligence groups, and criminal justice entities with access to confidential and sensitive law enforcement resources, for the purpose of obtaining confidential law enforcement information.

10. It was further part of the conspiracy that generally, after the conspiracy unlawfully obtained a victim's telephone call records, members of the conspiracy would use these records to make harassing phone calls or to harass the victim by uploading the records to a public website.

Overt Acts

11. In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere by members of the conspiracy:

(a) On or about July 17, 2015, co-conspirators CRACKA and ANDREW OTTO BOGGS, a/k/a "INCURSIO," exchanged direct messages on Twitter where CRACKA relayed that he had obtained the Social Security Number of a senior U.S. government official, and "jacked his comcast email so i can listen to his voicemail, look at his answered calls and...missed calls and control whats on his tv." CRACKA further stated, "i dont regret it, fuck the gov." In response, BOGGS asked whether CRACKA had used social engineering and BOGGS further encouraged the use of social engineering hacks. BOGGS then asked CRACKA whether CRACKA was interested in combining efforts to conduct computer hacks, stating, "We'll only be hitting governments and security firms. I'm waiting on our logo to be finished before we commence attacks on governments. :)" CRACKA responded, "Sure, I'd love to join."

(b) On or about October 12, 2015, CRACKA gained unauthorized access to Victim 1's online account with Verizon Communications ("Verizon") and changed the account password. Victim 1 was a senior U.S. Government official who worked and resided in the Eastern District of Virginia, who received Internet, telephone, and cable television services at his residence from Verizon.

(c) On or about October 12, 2015, during a private online discussion between BOGGS and CRACKA about Victim 1, BOGGS stated that he was “going to help [CRACKA] with Owning the [U.S. government agency affiliated with Victim 1],” and further stated, “If you need any publishing done, let me know. I’ll go Charlotte and use public wifi to publish the stolen information.”

(d) On or about October 13, 2015, CRACKA gained unauthorized access to Victim 1’s personal AOL email account and, among other things, changed the account password. The servers for AOL are located in the Eastern District of Virginia.

(e) Between on or about October 13, 2015, to on or about October 18, 2015, Victim 1 received multiple phone calls to his home in the Eastern District of Virginia and cellphone from CRACKA and/or other members of the conspiracy. The calls were harassing and derogatory in nature. During this period, other family members of Victim 1 located within the Eastern District of Virginia also received telephone calls from CRACKA and/or other members of the conspiracy that were harassing in nature.

(f) On or about October 19, 2015, CRACKA provided BOGGS with Victim 1’s personal AOL email address and other personally identifying information, as well as personal information belonging to Victim 1’s spouse.

(g) On or about October 20, 2015, defendant JUSTIN GRAY LIVERMAN, a/k/a “INCURSIO,” exchanged direct messages with CRACKA via Twitter where LIVERMAN congratulated CRACKA for gaining access to Victim 1’s online accounts. LIVERMAN subsequently used his Twitter and Facebook accounts to further harass Victim 1 by, among other things, posting screenshots of documents CRACKA unlawfully obtained from Victim 1’s personal online accounts.

(h) On or about November 18, 2015, BOGGS used Victim 1's personal email address to pose as Victim 1 in a communication with a computer security company. BOGGS then published on Twitter information about Victim 1 that he had obtained without authorization.

(i) On or about November 2, 2015, CRACKA provided LIVERMAN with Victim 2's cellphone number, which CRACKA had unlawfully obtained from Victim 2's personal online accounts. Victim 2 was a senior U.S. government official who worked for a federal law enforcement agency. Later that day, LIVERMAN paid an unlawful online service to dial Victim 2's phone number from spoofed and random phone numbers once an hour for 30 days, and to leave a threatening recorded message. LIVERMAN also used a disposable email address service to send a threatening and harassing text message to Victim 2's cellphone.

(j) On or about November 4, 2015, CRACKA informed LIVERMAN that he had used Victim 2's official credentials to obtain unauthorized access to the LEEP computer system. Later that day and at LIVERMAN's request, CRACKA sent LIVERMAN a list of information CRACKA had obtained through Victim 2's LEEP account – including names, phone numbers, and email addresses – relating to more than 80 police officers and law enforcement employees in the Miami area.

(k) On or about November 5, 2015, LIVERMAN used his @_D3F4ULT Twitter account to post about the conspiracy's hack into the LEEP database, and tagged co-conspirator BOGGS with BOGGS's Twitter account "@IncursioSubter."

(l) In or around November 2015, BOGGS requested from CRACKA Victim 2's login credentials for the LEEP database so that he could access the Joint Automated Booking System ("JABS") through LEEP. BOGGS gained or attempted to gain access to Victim 2's JABS account to access confidential law enforcement information.

(m) On or about November 21, 2015, BOGGS and CRACKA discussed regaining unauthorized access to the LEEP computer system. CRACKA asked BOGGS whether he should “add our aliases when i regain access?” BOGGS responded, “Yeah, add our aliases.”

(n) On or about December 11, 2015, per LIVERMAN’s request, CRACKA gained unauthorized access to Victim 3’s online account with Verizon. Victim 3 and his spouse, who was a senior U.S. government official, received telephone and cable television services from Verizon at their residence. LIVERMAN used login credentials that he received from CRACKA to make multiple attempts to gain unauthorized entry into Victim 3’s online Verizon account.

(o) On or about December 12, 2015, LIVERMAN asked CRACKA to call the cellphone number associated with Victim 3’s Verizon account, and LIVERMAN also placed a call to Victim 3’s residential phone number. Over the next few days, CRACKA called Victim 3’s cellphone and home phone multiple times, with the intent to harass Victim 3 and his spouse.

(p) On or about December 18, 2015, CRACKA sent LIVERMAN via Jabber a link to a news article about Victim 4, and stated, “[Victim 4’s] getting hacked.” Victim 4 was a senior U.S. government official who worked for a federal law enforcement agency and resided in the Eastern District of Virginia with her spouse, and who received Internet, telephone, and cable television services from Comcast Communications (“Comcast”) at her residence. LIVERMAN responded, “fuck yeah plz do.” CRACKA replied, “i’ll see what i can do :3.” Later in the conversation, LIVERMAN asked CRACKA whether he had uncovered Victim 4’s cellphone number, stating: “id loooove to phonebomb [Victim 4’s] voicemail ... and sms spam.” LIVERMAN later stated about Victim 4, “time to fuck her up.”

(q) On or about December 19, 2015, CRACKA informed LIVERMAN over

Jabber that he had gained access to Victim 4's online Comcast account. LIVERMAN responded, "roger that, set off the explosivees." CRACKA also informed LIVERMAN that he had accessed Victim 4's call records for her home in the Eastern District of Virginia, a copy of which LIVERMAN requested. Over the next few hours, LIVERMAN and CRACKA discussed different ways they could harass Victim 4 using the information they had unlawfully obtained from her Comcast account.

(r) On or about December 19, 2015, CRACKA altered the Comcast account settings for Victim 4's home in the Eastern District of Virginia by, among other things, resetting Victim 4's account password, resetting the passcode to Victim 4's voicemail, causing certain movies to play on the cable box at Victim 4's home in the Eastern District of Virginia, and renaming Victim 4's home cable boxes with derogatory and harassing terms.

(s) On or about December 19, 2015, Victim 4 received at least one harassing phone call from CRACKA.

(t) On or about December 26, 2015, CRACKA told LIVERMAN in a Jabber chat that he would target Victim 5's company. Victim 5 was the CEO of a company with an office in the Eastern District of Virginia. When LIVERMAN asked, "why them?" CRACKA responded, "im targeting them because they supply gov," to which LIVERMAN replied, "niice."

(u) On or about December 27, 2015, CRACKA informed LIVERMAN via Jabber that he had gained unauthorized access to a Facebook account belonging to Victim 5's spouse, and LIVERMAN and CRACKA discussed ways to harass Victim 5 using the account. That same day, CRACKA defaced the Facebook account belonging to Victim 5's spouse, and LIVERMAN and CRACKA used the account to stage a harassing conversation between LIVERMAN and Victim 5's spouse. Later that day, LIVERMAN used his pseudonymous

Twitter account @_D3F4ULT to tweet: “watching my ninja @[CRACKA’s Twitter account] destroy [Victim 5’s company] #CWA.”

(v) In or around January 2016, CRACKA gained unauthorized access to the U.S. government’s Case Information Management System (CIMS) by using government credentials that he unlawfully obtained. CIMS was a protected computer system run by the U.S. Department of Justice’s Civil Division. BOGGS agreed to upload information that CRACKA unlawfully obtained from the CIMS system to publicly accessible websites.

(w) In or around February 2016, BOGGS uploaded information that CRACKA unlawfully obtained from the CIMS computer system – including the names, telephone numbers, and email addresses of tens of thousands of Department of Justice and Department of Homeland Security employees – to multiple publicly accessible websites, and BOGGS encouraged others via Twitter to do the same.

(All in violation of Title 18, United States Code, Section 371.)

Dana J. Boente
United States Attorney

By: 

Maya D. Song
Jay V. Prabhu
Assistant United States Attorneys

Joseph V. Longobardo
Special Assistant United States Attorney (LT)